Application of constacyclic codes to quantum MDS codes

Chen, Bocong; Ling, San; Zhang, Guanghui

2015

Chen, B., Ling, S., & Zhang, G. (2015). Application of constacyclic codes to quantum MDS codes. IEEE transactions on information theory, 61(3), 1474-1484.

https://hdl.handle.net/10356/107237

https://doi.org/10.1109/TIT.2015.2388576

Application of Constacyclic Codes to Quantum MDS Codes

Bocong Chen, San Ling and Guanghui Zhang

***Abstract*—Quantum maximum-distance-separable (MDS) codes form an important class of quantum codes. To get q-ary quantum MDS codes, one of the effective ways is to find linear MDS codes C over $\mathbb{F}_{q^2}$ satisfying $C^{\perp_H} \subseteq C$, where $C^{\perp_H}$ denotes the Hermitian dual code of C. For a linear code C of length n over $\mathbb{F}_{q^2}$, we say that C is a dual-containing code if $C^{\perp_H} \subseteq C$ and $C \neq \mathbb{F}_{q^2}^n$. Several classes of new quantum MDS codes with relatively large minimum distance have been produced through dual-containing constacyclic MDS codes (see [15], [17], [24], [25]). These works motivate us to make a careful study on the existence conditions for dual-containing constacyclic codes. We obtain necessary and sufficient conditions for the existence of dual-containing constacyclic codes. Four classes of dual-containing constacyclic MDS codes are constructed and their parameters are computed. Consequently, quantum MDS codes are derived from these parameters. The quantum MDS codes exhibited here have minimum distance bigger than the ones available in the literature.**

***Index Terms*—quantum MDS code, cyclotomic coset, constacyclic code.**

I. INTRODUCTION

QUANTUM codes are useful in quantum computing and in quantum communications. Just as in the classical case, any q-ary quantum code has three parameters, the code length, the size of the code and the minimum distance. One of the principal problems in quantum error correction is to construct quantum codes with the best possible minimum distance. The CSS construction and its variants are frequently-used construction methods (see, [1]- [4], [6], [14]- [19], [21], [23], [28]- [35]). In practice, there have been a few experimental realizations of quantum codes up to some small lengths (see [12] and [32]).

Calderbank *et al.* in [7] discovered that we can construct quantum codes from classical self-orthogonal codes over $\mathbb{F}_2$ or $\mathbb{F}_4$ with respect to certain inner product. Thereafter, a lot of good quantum codes have been obtained by using classical error-correcting codes (see [8], [10], [11], [21], [24]).

We use $[[n,k,d]]_q$ to denote a q-ary quantum code of length n with size q^k and minimum distance d, where q is a prime power. It is well known that the parameters of an $[[n,k,d]]_q$ quantum code must satisfy the quantum Singleton bound: $2d \leq n-k+2$ (see [26] and [27]). A quantum code achieving this quantum Singleton bound is called a quantum maximum-distance-separable (MDS) code. Quantum information can be protected by encoding it into a quantum error-correcting code. Constructing good quantum error-correcting codes is thus of significance in theory and practice. However, it is not an easy task to construct quantum MDS codes with length $n > q+1$. Moreover, constructing quantum MDS codes with relatively large minimum distance turns out to be difficult. As mentioned in [22], except for some sparse lengths n such as $n = q^2+1, \frac{q^2+1}{2}$ and q^2, almost all known q-ary quantum MDS codes have minimum distance less than or equal to $\frac{q}{2}+1$.

In recent years, several quantum MDS codes have been obtained based on the Hermitian construction (see Section 2). The Hermitian construction and the quantum Singleton bound imply that we can obtain q-ary quantum MDS codes from linear MDS codes C over $\mathbb{F}_{q^2}$ satisfying $C^{\perp_H} \subseteq C$, where $C^{\perp_H}$ denotes the Hermitian dual code of C. From this idea, Grassl *et al.* [15] obtained q-ary quantum MDS codes of length q^2-1 from cyclic codes over $\mathbb{F}_{q^2}$. La Guardia in [17] constructed a class of quantum MDS codes through MDS cyclic codes. Kai and Zhu in [24] obtained two classes of quantum MDS codes by using negacyclic codes. Following that line of research, Kai *et al.* in [25] produced several quantum MDS codes based on constacyclic codes. As pointed out in [25], constacyclic codes are a good source for producing quantum MDS codes.

These works motivate us to make a careful study on the condition $C^{\perp_H} \subseteq C$ when C is a constacyclic code. For a linear code C of length n over $\mathbb{F}_{q^2}$, we say that C is a dual-containing code if $C^{\perp_H} \subseteq C$ and $C \neq \mathbb{F}_{q^2}^n$. We show that dual-containing λ-constacyclic codes over $\mathbb{F}_{q^2}$ exist only when the order of $\lambda \in \mathbb{F}_{q^2}^*$ is a divisor of $q+1$. Furthermore, we obtain elementary number-theoretic conditions for the existence of dual-containing constacyclic codes. This would help us to avoid unnecessary attempts in constructing dual-containing constacyclic codes. In particular, assuming that q is an odd prime power and $\lambda \in \mathbb{F}_{q^2}^*$ has order r, we show that if r is a divisor of $q+1$ and $2(q+1)$ divides rn, then dual-containing λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ always exist. In the light of this result, four classes of dual-containing MDS constacyclic codes are constructed and their parameters are computed. Consequently, quantum MDS codes are derived from these parameters. More precisely, we construct four classes of q-ary quantum MDS codes with the following parameters:

Bocong Chen is with the Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637616, Singapore (e-mail: bocong_chen@yahoo.com).

San Ling is with the Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637616, Singapore, (e-mail: lingsan@ntu.edu.sg).

Guanghui Zhang is with the School of Mathematical Sciences, Luoyang Normal University, Luoyang, Henan, 471022, China (e-mail: zghui2012@126.com).

(i)

$$\left[\left[\frac{q^2-1}{h}, \frac{q^2-1}{h}-2d+2, d\right]\right]_q$$

where q is an odd prime power, $h \in \{3,5,7\}$ is a divisor of $q+1$ and $2 \le d \le \frac{(q+1)(h+1)}{2h}-1$;

(ii)

$$\left[\left[2t(q-1), 2t(q-1)-2d+2, d\right]\right]_q$$

where q is an odd prime power with $8 \mid (q+1)$, t is an odd divisor of $q+1$ and $2 \le d \le 6t-1$;

(iii)

$$\left[\left[3(q-1), 3(q-1)-2d+2, d\right]\right]_q$$

where q is an odd prime power with $3^2 \mid (q+1)$ and $2 \le d \le \frac{q+5}{2}$;

(iv)

$$\left[\left[2^f s(q+1), 2^f s(q+1)-2d+2, d\right]\right]_q$$

where q is an odd prime power with $2^e \| (q-1)$ and $s \mid (q-1)$ (s odd), $0 \le f < e$ and $2 \le d \le \frac{q+1}{2}+2^f s$.

We mention that construction (iv) extends some results of [25]. Specifically, construction (iv) is a generalization of [25, Theorem 3.7] and [25, Theorem 3.10], which considered the cases $f=0$ and $f=1$, respectively. Moreover, taking $2^f s = \frac{q-1}{2}$ in construction (vi), we can reobtain [25, Theorem 3.2] directly. Comparing the parameters with all known quantum MDS codes, we find that these quantum MDS codes are new in the sense that their parameters are not covered by the codes available in the literature. Fixing the length and q, many of the new codes have minimum distance greater than the ones available in the literature.

This paper is organized as follows. In Section 2, basic notations and results about quantum codes and constacyclic codes are provided. In Section 3, necessary and sufficient conditions for the existence of dual-containing constacyclic codes are obtained. In Section 4, four classes of quantum MDS codes are constructed through constacyclic codes. The quantum MDS codes obtained are collected in Section 5, and the parameters of the new quantum MDS codes are compared with previously known quantum MDS codes.

II. Preliminaries

In this section, we review some basic notations and results about quantum codes and constacyclic codes. Throughout this paper, q denotes an odd prime power and $\mathbb{F}_{q^2}$ denotes the finite field with q^2 elements. We always assume that n is a positive integer relatively prime to q, i.e., $\gcd(n,q)=1$. As usual, for integers a and b, $a \mid b$ means that a divides b, $2^a \| b$ means that $2^a \mid b$ but $2^{a+1} \nmid b$. For any positive integer t, there is a unique nonnegative integer $\nu_2(t)$ such that $2^{\nu_2(t)} \| t$.

Let $\mathbb{F}_{q^2}^n$ be the $\mathbb{F}_{q^2}$-vector space of n-tuples. A *linear code* of length n over $\mathbb{F}_{q^2}$ is an $\mathbb{F}_{q^2}$-subspace of $\mathbb{F}_{q^2}^n$. A linear code of length n over $\mathbb{F}_{q^2}$ is called an $[n,k,d]$ code if its dimension is k and minimum Hamming distance is d.

Given two n-tuples $\mathbf{x}=(x_0,x_1,\cdots,x_{n-1}) \in \mathbb{F}_{q^2}^n$ and $\mathbf{y}=(y_0,y_1,\cdots,y_{n-1}) \in \mathbb{F}_{q^2}^n$, the *Hermitian inner product* is defined as

$$(\mathbf{x},\mathbf{y})_H = x_0\overline{y_0}+x_1\overline{y_1}+\cdots+x_{n-1}\overline{y_{n-1}}$$

where $\overline{y}=y^q$ for any $y \in \mathbb{F}_{q^2}$. For a linear code C of length n over $\mathbb{F}_{q^2}$, the Hermitian dual code of C is defined as

$$C^{\perp_H} = \left\{\mathbf{x} \in \mathbb{F}_{q^2}^n \;\middle|\; \sum_{i=0}^{n-1} x_i\overline{y_i}=0, \text{ for all } \mathbf{y} \in C\right\}.$$

If $C^{\perp_H} \subseteq C$ and $C \neq \mathbb{F}_{q^2}^n$, we say that C is a (Hermitian) *dual-containing code.*

The automorphism of $\mathbb{F}_{q^2}$ given by "$-$", $^-(x)=\overline{x}=x^q$ for any $x \in \mathbb{F}_{q^2}$, can be extended to an automorphism of $\mathbb{F}_{q^2}[X]$ in an obvious way:

$$\mathbb{F}_{q^2}[X] \longrightarrow \mathbb{F}_{q^2}[X], \quad \sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} \overline{a_i} X^i,$$

for any $a_0,a_1,\cdots,a_n$ in $\mathbb{F}_{q^2}$, which is also denoted by "$-$" for simplicity.

For a monic polynomial $f(X) \in \mathbb{F}_{q^2}[X]$ of degree k with $f(0) \neq 0$, its *reciprocal polynomial* $f(0)^{-1}X^k f(X^{-1})$ will be denoted by $f(X)^*$. Note that $f(X)^*$ is also a monic polynomial.

A. *Quantum codes*

A q-ary quantum code Q of length n and size K is a K-dimensional subspace of the q^n-dimensional Hilbert space $(\mathbb{C}^q)^{\otimes n}$. Let $k=\log_q(K)$. We use $[[n,k,d]]_q$ to denote a q-ary quantum code of length n with size q^k and minimum distance d. An important parameter of a quantum code is its minimum distance. If a quantum code has minimum distance d, then it can detect any $d-1$ and correct any $\lfloor \frac{d-1}{2} \rfloor$ errors. One of the principal problems in quantum coding theory is to construct quantum codes with the best possible minimum distance.

As mentioned previously, the parameters of an $[[n,k,d]]_q$ quantum code must satisfy the quantum Singleton bound (see [26] and [27]).

Proposition II.1. (**Quantum Singleton bound**) *Let Q be a q-ary $[[n,k,d]]_q$ quantum code. Then $2d \le n-k+2$.*

A quantum code achieving this quantum Singleton bound is called a *quantum maximum-distance-separable* (MDS) code. Ketkar *et al.* in [26] pointed out that, for any odd prime power q, if the classical MDS conjecture holds, then the length of nontrivial quantum MDS codes cannot exceed q^2+1. Constructing quantum MDS codes has become a hot research topic for quantum codes in recent years. The following is one of the most frequently-used construction methods (see [2]).

Proposition II.2. *If C is a q^2-ary $[n,k,d]$ linear code such that $C^{\perp_H} \subseteq C$, then there exists a q-ary quantum code with parameters $[[n,2k-n,\ge d]]_q$.*

As Proposition II.2 involves the Hermitian inner product, we refer to it as *the Hermitian construction*. The Hermitian construction suggests that we can obtain q-ary quantum codes from classical dual-containing linear codes over $\mathbb{F}_{q^2}$. Constacyclic codes form an important class of linear codes due to their good algebraic structures (e.g., see [9]). In this paper, we use the Hermitian construction to obtain quantum MDS codes through constacyclic codes.

B. Constacyclic codes

Let $\mathbb{F}_{q^2}^*$ denote the multiplicative group of nonzero elements of $\mathbb{F}_{q^2}$. For $\beta \in \mathbb{F}_{q^2}^*$, we denote by $\mathrm{ord}(\beta)$ the order of β in the group $\mathbb{F}_{q^2}^*$; then $\mathrm{ord}(\beta)$ is a divisor of q^2-1, and β is called a *primitive* $\mathrm{ord}(\beta)^{\mathrm{th}}$ *root of unity*.

For $\lambda \in \mathbb{F}_{q^2}^*$, a linear code C of length n over $\mathbb{F}_{q^2}$ is said to be λ-*constacyclic* if $(\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C$ for every $(c_0, c_1, \cdots, c_{n-1}) \in C$. When λ =1, λ-constacyclic codes are *cyclic codes*, and when $\lambda = -1$, λ-constacyclic codes are just *negacyclic codes*. Each codeword $\mathbf{c} = (c_0, c_1, \cdots, c_{n-1}) \in C$ is customarily identified with its polynomial representation $c(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$. In this way, every λ-constacyclic code C is identified with exactly one ideal of the quotient algebra $\mathbb{F}_{q^2}[X]/\langle X^n - \lambda\rangle$. We then know that C is generated uniquely by a monic divisor $g(X)$ of $X^n-\lambda$; in this case, $g(X)$ is called the *generator polynomial* of C and we write $C = \langle g(X)\rangle$. In particular, the irreducible factorization of $X^n - \lambda$ in $\mathbb{F}_{q^2}[X]$ determines all the λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$.

Let $\lambda \in \mathbb{F}_{q^2}^*$ be a primitive r^{th} root of unity. Then there exists a primitive rn^{th} root of unity (in some extension field of $\mathbb{F}_{q^2}$), say η, such that $\eta^n = \lambda$. The roots of $X^n - \lambda$ are precisely the elements η^{1+ri} for $0 \le i \le n-1$. Set $\theta_{r,n} = \{1 + ri \,|\, 0 \le i \le n-1\}$. The defining set of a constacyclic code $C = \langle g(X)\rangle$ of length n is the set $Z = \{j \in \theta_{r,n} \,|\, \eta^j \text{ is a root of } g(X)\}$. It is easy to see that the defining set Z is a union of some q^2-cyclotomic cosets modulo rn and $\dim_{\mathbb{F}_{q^2}}(C) = n - |Z|$ (see [37]).

The following result gives the generator polynomial of $C^{\perp_H}$, where C is a constacyclic code (e.g., see [37, Lemma 2.1(ii)]).

Lemma II.3. *Let $C = \langle g(X)\rangle$ be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$, where $g(X)$ is the generator polynomial of C. Let $h(X) = \frac{X^n-\lambda}{g(X)}$. Then the Hermitian dual code $C^{\perp_H}$ is a $\overline{\lambda}^{-1}$-constacyclic code with generator polynomial $\overline{h(X)^*}$.*

Remark II.4. *Let $f(X)$ be a monic polynomial in $\mathbb{F}_{q^2}[X]$ with $f(0) \neq 0$. It is readily seen that $\overline{f(X)^*} = \left(\overline{f(X)}\right)^*$. For simplicity we write $f(X)^\sigma = \overline{f(X)^*} = \overline{f(X)}^*$, namely σ can be regarded as the composition "$^- \circ ^*$". It is clear that $f(X)^{\sigma^2} = f(X)$.*

The proof of the following result is straight-forward, so we omit it here.

Lemma II.5. *Let α, β be nonzero elements of $\mathbb{F}_{q^2}$. Let $C_1 \neq \{0\}, C_2 \neq \{0\}$ be α- and β-constacyclic codes of length n over $\mathbb{F}_{q^2}$, respectively. If $C_1 \subseteq C_2$, $C_1 \neq \mathbb{F}_{q^2}[X]/\langle X^n - \alpha\rangle$ and $C_2 \neq \mathbb{F}_{q^2}[X]/\langle X^n - \beta\rangle$, then $\alpha = \beta$.*

As an immediate application of Lemmas II.3 and II.5, we have the following result.

Corollary II.6. *Let $\lambda \in \mathbb{F}_{q^2}^*$ be a primitive r^{th} root of unity and let C be a dual-containing λ-constacyclic code of length n over $\mathbb{F}_{q^2}$. We then have $\lambda = \overline{\lambda}^{-1}$, i.e., $r \mid (q+1)$.*

The next result presents a criterion to determine whether or not a given λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ is dual-containing (e.g., see [25, Lemma 2.2]).

Lemma II.7. *Let r be a positive divisor of $q+1$ and let $\lambda \in \mathbb{F}_{q^2}^*$ be of order r. Assume that C is a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set Z. Then C is a dual-containing code if and only if $Z \bigcap Z^{-q} = \emptyset$, where $Z^{-q} = \{-qz \pmod{rn} \,|\, z \in Z\}$.*

The following results are well known (see [5, Theorem 2.2] or [37, Theorem 4.1]).

Theorem II.8. ***(**BCH bound for constacyclic codes**)** *Let C be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$, where λ is a primitive r^{th} root of unity. Let η be a primitive rn^{th} root of unity in an extension field of $\mathbb{F}_{q^2}$ such that $\eta^n = \lambda$. Assume the generator polynomial of C has roots that include the set $\{\eta^{1+ri} \,|\, i_1 \le i \le i_1 + d - 2\}$. Then the minimum distance of C is at least d.*

Proposition II.9. ***(**Singleton bound**)** *Let C be a code of length n and minimum distance d over an alphabet of size a. Then $|C| \le a^{n-d+1}$. In particular, if C is an $[n, k, d]$ linear code over $\mathbb{F}_{q^2}$, then $k \le n - d + 1$.*

Some remarks are in order at this point. Theorem II.8 provides a useful method to construct constacyclic MDS codes: If the generator polynomial $g(X)$ has roots precisely equal to the set $\{\eta^{1+ri} \,|\, i_1 \le i \le i_1 + d - 1\}$, then the minimum distance of C is exactly equal to d. In particular, C is a constacyclic MDS code with parameters $[n, n-d+1, d]$. We will construct dual-containing constacyclic MDS codes based on these facts and Lemma II.7.

III. Existence conditions for dual-containing constacyclic codes

Assume that $\lambda \in \mathbb{F}_{q^2}$ is a primitive r^{th} root of unity. Clearly, r is a divisor of q^2-1. In particular, $\gcd(r, q) = 1$. To study dual-containing λ-constacyclic codes, we may assume first that $\lambda = \overline{\lambda}^{-1}$ by Corollary II.6, i.e., $r \mid (q+1)$.

For any monic irreducible factor $f(X) \in \mathbb{F}_{q^2}[X]$ of $X^n - \lambda$, $f(X)^\sigma$ is also a monic irreducible factor of $X^n - \lambda$ satisfying $f(X)^{\sigma^2} = f(X)$ (see Remark II.4). This implies that $X^n - \lambda$ can be factorized into distinct monic irreducible polynomials as follows

$$\begin{aligned} X^n - \lambda = & f_1(X)f_2(X)\cdots f_u(X) \\ & \cdot h_1(X)h_1^\sigma(X)h_2(X)h_2^\sigma(X)\cdots h_v(X)h_v^\sigma(X), \end{aligned}$$

where $f_i(X)$ $(1 \le i \le u)$ are distinct monic irreducible factors over $\mathbb{F}_{q^2}$ such that $f_i(X)^\sigma = f_i(X)$, while $h_j(X)$ and $h_j(X)^\sigma$ $(1 \le j \le v)$ are distinct monic irreducible factors over $\mathbb{F}_{q^2}$. As such, we have the following definition:

Definition III.1. *Let $f(X)$ be a monic polynomial in $\mathbb{F}_{q^2}[X]$ with $f(0) \neq 0$. We say that $f(X)$ is conjugate-self-reciprocal* *if $f(X)^\sigma = f(X)$. Otherwise, we say that $f(X)$ and $f(X)^\sigma$ form a conjugate-reciprocal polynomial pair.*

It should be pointed out that u may be equal to 0, namely no irreducible factor of $X^n - \lambda$ over $\mathbb{F}_{q^2}$ is conjugate-self-reciprocal. Likewise, it is possible that $v = 0$, namely every irreducible factor of $X^n - \lambda$ over $\mathbb{F}_{q^2}$ is conjugate-self-reciprocal.

Let $C = \langle g(X) \rangle$ be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$, where $g(X)$ is a monic divisor of $X^n - \lambda$. We may assume, therefore, that

$$\begin{aligned} g(X) = & f_1(X)^{a_1} \cdots f_u(X)^{a_u} \\ & \cdot h_1(X)^{b_1} (h_1^\sigma(X))^{c_1} \cdots h_v(X)^{b_v} (h_v^\sigma(X))^{c_v} \end{aligned}$$

where $0 \le a_i \le 1$ for each i, and $0 \le b_j, c_j \le 1$ for each j. Then the generator polynomial of $C^{\perp_H}$ is

$$\begin{aligned} h(X)^\sigma = & \overline{h(X)^*} \\ = & f_1(X)^{1-a_1} \cdots f_u(X)^{1-a_u} \cdot h_1(X)^{1-c_1} (h_1^\sigma(X))^{1-b_1} \\ & \cdots \cdot h_v(X)^{1-c_v} (h_v^\sigma(X))^{1-b_v}. \end{aligned}$$

By Lemma II.3, C satisfies $C^{\perp_H} \subseteq C$ if and only if $g(X) \mid h(X)^\sigma$, i.e.,

$$\begin{cases} 2a_i \le 1, & \text{for each } i, \\ b_j + c_j \le 1, & \text{for each } j. \end{cases} \tag{III.1}$$

It follows that $C = \langle g(X) \rangle$ satisfies $C^{\perp_H} \subseteq C$ if and only if

$$C = \left\langle h_1(X)^{b_1} (h_1^\sigma(X))^{c_1} \cdots h_v(X)^{b_v} (h_v^\sigma(X))^{c_v} \right\rangle$$

where $0 \le b_j, c_j \le 1$ and $b_j + c_j \le 1$ for each j. This discussion leads to the following result.

Theorem III.2. *Let $\lambda \in \mathbb{F}_{q^2}^*$ satisfy $\lambda = \overline{\lambda}^{-1}$. Dual-containing λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ exist if and only if $v > 0$, i.e., there exists at least one conjugate-reciprocal polynomial pair among the monic irreducible factors of $X^n - \lambda$ over $\mathbb{F}_{q^2}$.*

In the rest of this section, we aim to obtain more simplified criteria for the existence of dual-containing λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$.

It is well known that the irreducible factors of $X^{rn} - 1$ over $\mathbb{F}_{q^2}$ can be described via the q^2-cyclotomic cosets modulo rn (see [20, Theorem 4.1.1]): Assume that $\Omega = \{i_0 = 0, i_1 = 1, i_2, \cdots, i_\rho\}$ is a set of representatives of the q^2-cyclotomic cosets modulo rn. Let C_{i_j} be the q^2-cyclotomic coset modulo rn containing i_j for $0 \le j \le \rho$. We then know that

$$X^{rn} - 1 = M_{i_0}(X) M_{i_1}(X) \cdots M_{i_\rho}(X) \tag{III.2}$$

with

$$M_{i_j}(X) = \prod_{s \in C_{i_j}} (X - \eta^s), \qquad j = 0, \cdots, \rho,$$

all being monic irreducible in $\mathbb{F}_{q^2}[X]$, where η is a primitive rn^{th} root of unity over some extension field of $\mathbb{F}_{q^2}$ such that $\eta^n = \lambda$. Since $X^n - \lambda$ is a divisor of $X^{rn} - 1$ in $\mathbb{F}_{q^2}[X]$, we can find a subset Δ of Ω such that

$$X^n - \lambda = \prod_{e \in \Delta} M_e(X). \tag{III.3}$$

Set $\mathcal{O}_{r,n} = \{C_j \mid j \in \Delta\}$. We also see that $C_{i_1} = C_1 \in \mathcal{O}_{r,n}$. We can now translate Theorem III.2 into the language of q^2-cyclotomic cosets modulo rn.

Lemma III.3. *Let $\lambda \in \mathbb{F}_{q^2}^*$ be of order r satisfying $\lambda = \overline{\lambda}^{-1}$. There exists a dual-containing λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ if and only if there exists $C_{e_0} \in \mathcal{O}_{r,n}$ such that $C_{e_0} \ne C_{-qe_0}$, where C_{e_0} and C_{-qe_0} denote the q^2-cyclotomic cosets modulo rn containing e_0 and $-qe_0$, respectively.*

Proof: Let $M_j(X) = \prod_{i \in C_j} (X - \eta^i)$ be the minimal polynomial of η^j over $\mathbb{F}_{q^2}$. Note that $M_j(X)^* = M_{-j}(X)$. Combining Theorem III.2 with (III.3), it suffices to prove that $\overline{M_j(X)} = M_{qj}(X)$. For this purpose, we only need to show that η^{qj} is a root of $\overline{M_j(X)}$. Assume that $M_j(X) = a_0 + a_1 X + \cdots + a_t X^t$ with $a_0, a_1, \cdots, a_t \in \mathbb{F}_{q^2}$. Thus $\overline{M_j(X)} = \overline{a_0} + \overline{a_1} X + \cdots + \overline{a_t} X^t$. Obviously $\overline{M_j}(\eta^{qj}) = 0$, since

$$\begin{aligned} \overline{M_j}(\eta^{qj}) &= \overline{a_0} + \overline{a_1} \eta^{qj} + \cdots + \overline{a_t} (\eta^{qj})^t \\ &= \left(a_0 + a_1 \eta^j + \cdots + a_t \eta^{tj}\right)^q = M_j(\eta^j)^q = 0. \end{aligned}$$

■

Let $\lambda \in \mathbb{F}_{q^2}^*$ be of order r satisfying $\lambda = \overline{\lambda}^{-1}$. Write $rn = 2^{\nu_2(rn)} p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, where p_j are distinct odd primes and k_j are positive integers for $1 \le j \le s$. Let $\mathbb{Z}_m^*$ denote the multiplicative group of all residue classes modulo m which are coprime with m, and let $\mathrm{ord}_{p_j^{k_j}}(q)$ denote the multiplicative order of $q \in \mathbb{Z}_{p_j^{k_j}}^*$, $1 \le j \le s$. We assert that $\nu_2\big(\mathrm{ord}_{p_j^{k_j}}(q)\big) = \nu_2\big(\mathrm{ord}_{p_j}(q)\big)$ for $1 \le j \le s$. Indeed, consider the natural surjective homomorphism $\pi : \mathbb{Z}_{p_j^{k_j}}^* \to \mathbb{Z}_{p_j}^*$, $x \pmod{p_j^{k_j}} \mapsto x \pmod{p_j}$. We then know that $\mathrm{ord}_{p_j}(q)$ is exactly equal to the order of $qKer\pi$ in the factor group $\mathbb{Z}_{p_j^{k_j}}^*/Ker\pi$, which is also equal to the smallest positive integer k such that $q^k \in Ker\pi$. Now the desired result follows from the fact that $Ker\pi$ is a group of odd order.

The next two results give existence conditions for dual-containing λ-constacyclic codes.

Theorem III.4. *Let r, n be positive integers with $\gcd(n, q) = 1$ and $r \mid (q+1)$. Suppose*

$$rn = 2^{\nu_2(rn)} p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$$

where p_j are distinct odd primes and k_j are positive integers for $1 \le j \le s$. We assume further that $\nu_2(rn) \le 1$. Then dual-containing λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ exist if and only if one of the following statements holds:

- **(i)** *There exists an integer t, $1 \le t \le s$, such that $\mathrm{ord}_{p_t}(q)$ is odd.*
- **(ii)** $\nu_2\big(\mathrm{ord}_{p_1}(q)\big) = \nu_2\big(\mathrm{ord}_{p_2}(q)\big) = \cdots = \nu_2\big(\mathrm{ord}_{p_s}(q)\big) \ge 2$.
- **(iii)** *The integer $s \ge 2$, $\mathrm{ord}_{p_j}(q)$ is even for all $1 \le j \le s$, and there exist distinct integers j_1, j_2 with $1 \le j_1, j_2 \le s$ such that $\nu_2\big(\mathrm{ord}_{p_{j_1}}(q)\big) \ne \nu_2\big(\mathrm{ord}_{p_{j_2}}(q)\big)$.*

Proof: Supposing that one of the above three conditions holds true, we work by contradiction to show that dual-containing λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ exist. By Lemma III.3, we can suppose that $C_e = C_{-qe}$ for any

$C_e \in \mathcal{O}_{r,n}$, where C_e denotes the q^2-cyclotomic coset modulo rn containing e. This leads to $C_1 = C_{-q}$ since $C_1 \in \mathcal{O}_{r,n}$, which implies that an integer i_0' can be found such that $q^{1+2i_0'} \equiv -1 \pmod{rn}$. Let $i_0 = 2i_0' + 1$, and thus $q^{i_0} \equiv -1 \pmod{rn}$. Clearly, i_0 is odd.

Assume that (i) holds. There is no loss of generality to assume that $\mathrm{ord}_{p_1}(q)$ is odd. It follows from $q^{i_0} \equiv -1 \pmod{p_1}$ that $q^{2i_0} \equiv 1 \pmod{p_1}$. Hence $\mathrm{ord}_{p_1}(q) \mid i_0$ as $\mathrm{ord}_{p_1}(q)$ is odd. This leads to $q^{i_0} \equiv 1 \pmod{p_1}$, a contradiction.

Assume that (ii) holds. In particular, $\nu_2\big(\mathrm{ord}_{p_1}(q)\big) \geq 2$. Recall that $\nu_2\big(\mathrm{ord}_{p_1^{k_1}}(q)\big) = \nu_2\big(\mathrm{ord}_{p_1}(q)\big)$. From $q^{i_0} \equiv -1 \pmod{p_1^{k_1}}$, we deduce that $q^{2i_0} \equiv 1 \pmod{p_1^{k_1}}$. Hence, $\mathrm{ord}_{p_1^{k_1}}(q)$ divides $2i_0$, which implies that i_0 is even. This is a contradiction.

Now we assume that (iii) holds. Without loss of generality, we may assume that $\nu_2\big(\mathrm{ord}_{p_1}(q)\big) > \nu_2\big(\mathrm{ord}_{p_2}(q)\big) \geq 1$. From $q^{i_0} \equiv -1 \pmod{p_j^{k_j}}$ for all $1 \leq j \leq s$, we have $q^{2i_0} \equiv 1 \pmod{p_j^{k_j}}$. Thus, $\mathrm{ord}_{p_j^{k_j}}(q)$ is a divisor of $2i_0$, so $\mathrm{ord}_{p_j^{k_j}}(q)/2$ divides i_0 for all $1 \leq j \leq s$. In particular, $\mathrm{ord}_{p_1^{k_1}}(q)/2$ is a divisor of i_0. Combining this fact with the hypothesis $\nu_2\big(\mathrm{ord}_{p_1}(q)\big) > \nu_2\big(\mathrm{ord}_{p_2}(q)\big) \geq 1$, it follows that i_0 is even, a contradiction again.

Conversely, assume that dual-containing λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ exist. We assume further that neither (i) nor (iii) holds. Then $\nu_2\big(\mathrm{ord}_{p_j}(q)\big) \geq 1$ for all $1 \leq j \leq s$. If $s = 1$, we need to show that $\nu_2\big(\mathrm{ord}_{p_1}(q)\big) > 1$. If $s \geq 2$, we know that $\nu_2\big(\mathrm{ord}_{p_1}(q)\big) = \nu_2\big(\mathrm{ord}_{p_2}(q)\big) = \cdots = \nu_2\big(\mathrm{ord}_{p_s}(q)\big) > 0$. We are thus left to prove that $\nu_2\big(\mathrm{ord}_{p_1}(q)\big) = \nu_2\big(\mathrm{ord}_{p_2}(q)\big) = \cdots = \nu_2\big(\mathrm{ord}_{p_s}(q)\big) = x > 1$. Suppose otherwise that $x = 1$. For any $1 \leq j \leq s$, let y_j be a positive integer such that $\mathrm{ord}_{p_j^{k_j}}(q) = 2y_j$. Thus, $q^{2y_j} \equiv 1 \pmod{p_j^{k_j}}$ for any j. From the fact that $\mathbb{Z}^*_{p_j^{k_j}}$ is a cyclic group whose unique element of order 2 is $[-1]_{p_j^{k_j}}$, where $[-1]_{p_j^{k_j}}$ denotes the residue class modulo $p_j^{k_j}$ containing -1, it follows that $q^{y_j} \equiv -1 \pmod{p_j^{k_j}}$. Let $y = \prod_{j=1}^{s} y_j$. We get $q^y \equiv -1 \pmod{p_j^{k_j}}$ for all $1 \leq j \leq s$. Therefore, $q^y \equiv -1 \pmod{p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}}$. This leads to $q^y \equiv -1 \pmod{rn}$, as $\nu_2(r) + \nu_2(n) \leq 1$. We get the desired contradiction, since we would obtain $C_1 = C_{-q}$. ∎

Finally we consider the remaining case: $\nu_2(rn) \geq 2$.

Theorem III.5. *Let r, n be positive integers with $\gcd(n, q) = 1$ and $r \mid (q+1)$. Suppose*

$$rn = 2^{\nu_2(rn)} p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$$

where p_j are distinct odd primes and k_j are positive integers for $1 \leq j \leq s$. We assume further that $\nu_2(rn) \geq 2$. Then dual-containing λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ exist if and only if one of the following statements holds:

- **(i)** $q \equiv 1 \pmod 4$.
- **(ii)** $q \equiv -1 \pmod 4$ *and* $\nu_2(rn) > e$, *where e is the positive integer such that* $2^e \| (q+1)$.
- **(iii)** *There exists an integer j_0, $1 \leq j_0 \leq s$, such that* $\mathrm{ord}_{p_{j_0}}(q)$ *is odd.*
- **(iv)** $\mathrm{ord}_{p_j}(q)$ *is even for all $1 \leq j \leq s$ and there exists some integer j_1, $1 \leq j_1 \leq s$, such that 4 divides* $\mathrm{ord}_{p_{j_1}}(q)$.

Proof: By Lemma III.3, we know that dual-containing λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ do not exist if and only if $C_1 = C_{-q}$, where C_1 and C_{-q} denote the q^2-cyclotomic cosets modulo rn containing 1 and $-q$, respectively.

Suppose that one of the above four conditions holds true, and we proceed by way of contradiction. It follows from $C_1 = C_{-q}$ that an odd integer i_0 can be found such that $q^{i_0} \equiv -1 \pmod{rn}$.

Assume that (i) holds. We have $q^{i_0} \equiv -1 \pmod{2^{\nu_2(r)+\nu_2(n)}}$, since $2^{\nu_2(r)+\nu_2(n)}$ divides rn. By assumption $\nu_2(r) + \nu_2(n) \geq 2$, so $q^{i_0} \equiv -1 \pmod 4$. This contradicts $q \equiv 1 \pmod 4$.

Assume that (ii) holds. Write $q + 1 = 2^e f$, where f is an odd positive integer. By assumption $\nu_2(r) + \nu_2(n) > e$, then $q^{i_0} \equiv -1 \pmod{2^{e+1}}$. Let $i_0 = 2i_0' + 1$. Since $q \equiv -1 \pmod{2^e}$, it follows that $q^2 \equiv 1 \pmod{2^{e+1}}$, which gives $q^{2i_0'} \equiv 1 \pmod{2^{e+1}}$. Thus $q^{2i_0'+1} \equiv q \pmod{2^{e+1}}$, namely $q^{i_0} \equiv q \pmod{2^{e+1}}$. Combining with $q^{i_0} \equiv -1 \pmod{2^{e+1}}$, we get $q \equiv -1 \pmod{2^{e+1}}$. However, this contradicts the fact that $q + 1 = 2^e f$ with f odd.

Assume that (iii) holds. There is no loss of generality to assume that $\mathrm{ord}_{p_1}(q)$ is odd. From $q^{i_0} \equiv -1 \pmod{rn}$, we see that $q^{i_0} \equiv -1 \pmod{p_1}$ and so $q^{2i_0} \equiv 1 \pmod{p_1}$. Since $\mathrm{ord}_{p_1}(q) \mid 2i_0$, we have $\mathrm{ord}_{p_1}(q) \mid i_0$. Thus $q^{i_0} \equiv 1 \pmod{p_1}$, a contradiction.

Assume that (iv) holds. Recall that $\nu_2\big(\mathrm{ord}_{p_1^{k_1}}(q)\big) = \nu_2\big(\mathrm{ord}_{p_1}(q)\big)$. Suppose 4 is a divisor of $\mathrm{ord}_{p_1}(q)$. Obviously $q^{2i_0} \equiv 1 \pmod{p_1^{k_1}}$. It follows that $\mathrm{ord}_{p_1^{k_1}}(q)$ is a divisor of $2i_0$ and then i_0 is even. This is a contradiction.

Now, suppose that dual-containing λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ exist. Assume further that (i), (ii) and (iii) do not hold. We need to show that (iv) holds. Since (iii) does not hold, $\mathrm{ord}_{p_j}(q)$ is even for all j. Assume, by way of contradiction, that $\mathrm{ord}_{p_j}(q)$ is even but not divisible by 4 for all $1 \leq j \leq s$, i.e., $x_j = 1$ for all $1 \leq j \leq s$. It follows from $q^{2y_j} \equiv 1 \pmod{p_j^{k_j}}$ that $q^{y_j} \equiv -1 \pmod{p_j^{k_j}}$. Let $y = \prod_{j=1}^{s} y_j$. We get $q^y \equiv -1 \pmod{p_j^{k_j}}$ for all $1 \leq j \leq s$. Therefore, $q^y \equiv -1 \pmod{p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}}$. The assumption that neither (i) nor (ii) holds true implies that $2^{\nu_2(r)+\nu_2(n)} \mid (q+1)$. It follows that $q^y \equiv -1 \pmod{2^{\nu_2(r)+\nu_2(n)}}$, since y is an odd positive integer. Hence $q^y \equiv -1 \pmod{rn}$. This gives the desired contradiction. ∎

Example III.6. *Let $q = 11$, then $q^2 = 11^2$. Suppose $\mathbb{F}^*_{11^2} = \langle \theta \rangle$. Let $\lambda = \theta^{10}$, then $r = 12$. By Theorem III.5, dual-containing λ-constacyclic codes of length 27 over $\mathbb{F}_{121}$ do not exist. This is because $rn = 324 = 2^2 \cdot 3^4$, $\nu_2(rn) \geq 2$ and $q = 11 \equiv -1 \pmod 4$, but $\nu_2(rn) = e = 2$, and $\mathrm{ord}_3(11) = 2$.*

Example III.7. *Let $q = 3^2$, then $q^2 = 3^4$. Suppose $\mathbb{F}^*_{3^4} = \langle \theta \rangle$. Let $\lambda = \theta^8$, then $r = 10$.*

(1) *By Theorem III.4, dual-containing λ-constacyclic codes of length 5 over $\mathbb{F}_{3^4}$ do not exist. This is because $rn = 50 = 2 \cdot 5^2$, $\nu_2(rn) \leq 1$ and $\mathrm{ord}_5(9) = 2$.*

(2) *By Theorem III.5, dual-containing λ-constacyclic codes of length* 10 *over* $\mathbb{F}_{3^4}$ *exist. In fact, since* $rn = 100 = 2^2 \cdot 5^2$*, then* $\nu_2(rn) \geq 2$ *and* $q = 9 \equiv 1 \pmod 4$.

Applying Theorem III.5, we have the following result.

Corollary III.8. *Let q be an odd prime power. Let r be a positive integer dividing $q+1$, and let $n > 1$ be a positive integer satisfying $2(q+1) \mid rn$ and $rn \mid (q^2-1)$. Assume that $\lambda \in \mathbb{F}_{q^2}^*$ is of order r. Then dual-containing λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ exist.*

Proof: It is clear that 4 divides rn. If $q \equiv 1 \pmod 4$, then we know from Theorem III.5(i) that the desired result follows. Otherwise, $q \equiv -1 \pmod 4$. In this case, Theorem III.5(ii) is satisfied. ■

IV. New quantum MDS codes

In this section, four classes of dual-containing MDS constacyclic codes are constructed and their parameters are computed. Consequently, new quantum MDS codes are derived from these parameters. In the light of Corollary III.8, we construct dual-containing MDS λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ satisfying $2(q+1) \mid rn$ and $rn \mid (q^2-1)$, where r is the order of λ. In order to obtain suitable defining sets algebraically, we first try to compute many small examples. We thus have a list of Hermitian dual-containing MDS constacyclic codes. Comparing these parameters carefully, our theorems are then generalized from these examples.

A. New quantum MDS codes of length $\frac{q+1}{h}(q-1)$ with $h \in \{3,5,7\}$

Let $h \in \{3,5,7\}$ and let q be an odd prime power with $h \mid (q+1)$. Suppose $n = \frac{q^2-1}{h}$ and $r = h$. Let $\lambda \in \mathbb{F}_{q^2}$ be a primitive r^{th} root of unity. Corollary III.8 guarantees that dual-containing λ-constacyclic codes of length $n = \frac{q^2-1}{h}$ over $\mathbb{F}_{q^2}$ exist. It is clear that $rn = q^2-1$, and hence every q^2-cyclotomic coset modulo rn contains exactly one element. Let C be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set

$$Z = \Big\{1 + hi \,\Big|\, \frac{(h-1)(q+1)}{2h} \leq i \leq q-2\Big\}. \tag{IV.1}$$

It is easy to see that $|Z| = \frac{h+1}{2} \cdot \frac{q+1}{h} - 2$. Thus, C is an MDS λ-constacyclic code with parameters $[n, n - \frac{(q+1)(h+1)}{2h} + 2, \frac{(q+1)(h+1)}{2h} - 1]$. We show now that C is a dual-containing code.

Lemma IV.1. *Let $h \in \{3,5,7\}$ and let q be an odd prime power with $h \mid (q+1)$. If C is a λ-constacyclic code of length $n = \frac{q^2-1}{h}$ over $\mathbb{F}_{q^2}$ with defining set Z as in (IV.1), then C is a dual-containing code.*

Proof: Suppose otherwise that C is not a dual-containing code. It follows from Lemma II.7 that $Z \bigcap Z^{-q} \neq \emptyset$. Hence, two integers i, j with $\frac{(h-1)(q+1)}{2h} \leq i, j \leq q-2$ can be found such that

$$-q(1+hi) \equiv 1 + hj \pmod{q^2-1}. \tag{IV.2}$$

If $i = j$, then $-q(1+hi) \equiv 1 + hi \pmod{q^2-1}$. Thus $(q-1) \mid (1+hi)$. Since

$$\begin{aligned}\frac{h-1}{2}(q-1) &< 1 + h \cdot \frac{(h-1)(q+1)}{2h} \\ &\leq 1 + hi \leq 1 + h(q-2) < h(q-1),\end{aligned}$$

we can assume, therefore, that $1+hi = k(q-1)$, where k is an integer with $\frac{h+1}{2} \leq k \leq h-1$. Then $hi = k(q+1) - (1+2k)$. Hence, $h \mid (1+2k)$. If $h = 3$, then $k = 2$. This implies $3 \mid 5$, which is impossible. Similar arguments show that neither $h = 5$ nor $h = 7$ is possible. We get a desired contradiction.

Without loss of generality, we may assume that $i > j$. By Equation (IV.2), we have $-q(1+hi) \equiv 1 + hj \pmod{q-1}$ and that $-q(1+hi) \equiv 1 + hj \pmod{q+1}$, i.e., $(q-1) \mid (hi + hj + 2)$ and $(q+1) \mid (hi - hj)$. Note that

$$\begin{aligned}(h-1)(q-1) &< 2 + 2h \cdot \frac{(h-1)(q+1)}{2h} \\ &\leq hi + hj + 2 \leq 2h(q-2) + 2 < 2h(q-1).\end{aligned}$$

Write $hi + hj + 2 = \ell_2(q-1)$, where $h \leq \ell_2 \leq 2h-1$. Thus $hi + hj = \ell_2(q+1) - 2(1+\ell_2)$. Therefore $h \mid 2(1+\ell_2)$, which implies that $h \mid (1+\ell_2)$. It follows from $h+1 \leq 1+\ell_2 \leq 2h$ that $1+\ell_2 = 2h$, i.e., $\ell_2 = 2h-1$. On the other hand,

$$\begin{aligned}0 &< hi - hj \leq h(q - 2 - \frac{(h-1)(q+1)}{2h}) \\ &< h\big((q+1) - \frac{(h-1)(q+1)}{2h}\big) = (q+1) \cdot \frac{h+1}{2}.\end{aligned}$$

We then have $hi - hj = \ell_1(q+1)$, where $1 \leq \ell_1 \leq \frac{h-1}{2}$.

Now from $hi - hj = \ell_1(q+1)$ and $hi + hj + 2 = (2h-1)(q-1)$, it follows that $2hi = (2h-1+\ell_1)(q+1) - 4h$. If $h = 3$, then $\ell_1 = 1$ and thus $i = q-1$. This is a contradiction, since $i \leq q-2$ by assumption. If $h = 5$, then $1 \leq \ell_1 \leq 2$ and $i = (9+\ell_1)\frac{q+1}{10} - 2 > q-2$, which also yields a contradiction. Similar argument shows that $h = 7$ is impossible as well. This completes the proof. ■

Using the Hermitian construction and the quantum Singleton bound, we have the following quantum MDS codes.

Theorem IV.2. *Let $h \in \{3,5,7\}$ and let q be an odd prime power with $h \mid (q+1)$. Then there exist quantum MDS codes with parameters $[[\frac{q^2-1}{h}, \frac{q^2-1}{h} - 2d + 2, d]]_q$, where $2 \leq d \leq \frac{(q+1)(h+1)}{2h} - 1$.*

Proof: Let $n = \frac{q^2-1}{h}$ and $r = h$. Let $\lambda \in \mathbb{F}_{q^2}$ be a primitive r^{th} root of unity. Recall that every q^2-cyclotomic coset modulo rn contains precisely one element. We assume that $\mathcal{C}_\delta$ is a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set

$$\mathcal{Z}_\delta = \Big\{1 + h\Big(\frac{(h-1)(q+1)}{2h} + i\Big) \,\Big|\, 0 \leq i \leq \delta - 1\Big\} \tag{IV.3}$$

where δ is a positive integer with $1 \leq \delta \leq \frac{(q+1)(h+1)}{2h} - 2$. Clearly, $\mathcal{Z}_\delta$ is a subset of Z where Z is given in (IV.1). By Lemma IV.1, we have $\mathcal{Z}_\delta \bigcap \mathcal{Z}_\delta^{-q} = \emptyset$. It follows that $\mathcal{C}_\delta$ is a dual-containing code with parameters $[n, n-d+1, d]$, where d is a positive integer with $d = \delta + 1$. Using the Hermitian construction and the quantum Singleton bound, we can obtain

q	$[[n,k,d]]_q$	d
11	$[[40,40-2d+2,d]]_{11}$	$2\le d\le 7$
17	$[[96,96-2d+2,d]]_{17}$	$2\le d\le 11$
23	$[[176,176-2d+2,d]]_{23}$	$2\le d\le 15$
9	$[[16,16-2d+2,d]]_{9}$	$2\le d\le 5$
13	$[[24,24-2d+2,d]]_{13}$	$2\le d\le 7$
27	$[[104,104-2d+2,d]]_{27}$	$2\le d\le 15$

TABLE I
QUANTUM MDS CODES

a quantum MDS code with parameters $[[\frac{q^2-1}{h}, \frac{q^2-1}{h}-2d+2,d]]_q$. ∎

Example IV.3. *In Table I, we list some quantum MDS codes obtained from Theorem IV.2.*

B. New quantum MDS codes of length $2t(q-1)$

Let q be an odd prime power with $8\mid(q+1)$. Let t be an odd divisor of $q+1$, $n=2t(q-1)$ and $r=\frac{q+1}{2t}$. Clearly, $q\ge 7$ and $r\ge 4$. We now obtain q-ary quantum MDS codes of length n through λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$, where $\lambda\in\mathbb{F}_{q^2}$ is a primitive r^{th} root of unity.

Let C be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set

$$Z=\Big\{1+ri\,\Big|-(2t-1)\le i\le 4t-2\Big\}. \tag{IV.4}$$

It follows from $2rt=q+1$ and $q\ge 7$ that $0<1+r(4t-2)<\frac{q^2-1}{2}$ and $-\frac{q^2-1}{2}<1-r(2t-1)<0$. Then, $|Z|=6t-2$. The next result shows that C is a dual-containing code.

Lemma IV.4. *If C is a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set Z as in (IV.4), then C is a dual-containing code.*

Proof: Since $8\mid(q+1)$ and $t\mid(q+1)$ with t being odd, we can assume that $q+1=8kt$, where k is an integer. Suppose that C is not a dual-containing code. By Lemma II.7, we have $Z\bigcap Z^{-q}\neq\emptyset$. Hence, two integers i,j with $-(2t-1)\le i,j\le 4t-2$ can be found such that

$$-q(1+ri)\equiv 1+rj \pmod{q^2-1}. \tag{IV.5}$$

If $i=j$, then $-q(1+ri)\equiv 1+ri \pmod{q^2-1}$, which gives $(q-1)\mid(1+ri)$. Let $1+ri=\ell(q-1)$, for some integer ℓ. Note that $r=\frac{q+1}{2t}=4k$. Thus $1+ri=1+4ki=\ell(8kt-2)$, i.e., $1=2(4\ell kt-\ell-2ki)$. This is a contradiction.

Without loss of generality, we may assume that $i>j$. By Equation (IV.5), $-q(1+ri)\equiv 1+rj \pmod{q-1}$ and $-q(1+ri)\equiv 1+rj \pmod{q+1}$, i.e., $(q-1)\mid\big(r(i+j)+2\big)$ and $(q+1)\mid r(i-j)$. Recall that $r=\frac{q+1}{2t}\ge 4$. We have

$$\begin{aligned}-2(q-1)&<-2q+2r=-2r(2t-1)+2\\ &\le r(i+j)+2\le\frac{q+1}{2t}(8t-4)+2\\ &=4q-4r+6<4(q-1)\end{aligned}$$

and

$$\begin{aligned}0<r(i-j)&\le\frac{q+1}{2t}(4t-2+2t-1)=\frac{q+1}{2t}(6t-3)\\ &<3(q+1).\end{aligned}$$

q	t	$[[n,k,d]]_q$	d
7	1	$[[12,12-2d+2,d]]_7$	$2\le d\le 5$
23	3	$[[132,132-2d+2,d]]_{23}$	$2\le d\le 17$

TABLE II
QUANTUM MDS CODES

Write $r(i+j)+2=\ell_1(q-1)$ and $r(i-j)=\ell_2(q+1)$, where $-1\le\ell_1\le 3$ and $1\le\ell_2\le 2$. Thus, $2ri=\ell_1(q-1)-2+\ell_2(q+1)=(q+1)(\ell_1+\ell_2)-2(1+\ell_1)$. It follows that $r\mid(1+\ell_1)$. By $4\mid r$, we have $4\mid(1+\ell_1)$. Since $\ell_1\in\{-1,0,1,2,3\}$, we obtain $\ell_1=-1$ or 3.

If $\ell_1=-1$, then $2rj=\ell_1(q-1)-\ell_2(q+1)-2=-(1+\ell_2)(q+1)$, which gives $j=-(1+\ell_2)t$. Since $\ell_2\in\{1,2\}$, we have $j=-2t$ or $-3t$, contradicting the assumption that $j\ge-(2t-1)$.

If $\ell_1=3$, then $2ri=(q+1)(\ell_2+3)-8$. It follows that $2r\mid 8$, which forces $r=4$. We then have $i=t(\ell_2+3)-1$. Since $\ell_2\in\{1,2\}$, we get $i=4t-1$ or $5t-1$, contradicting the assumption $i\le 4t-2$. ∎

Using the Hermitian construction, we have the following quantum MDS codes.

Theorem IV.5. *Let q be an odd prime power with $8\mid(q+1)$. Let t be an odd divisor of $q+1$. Then, there exists a quantum MDS code with parameters $[[2t(q-1),2t(q-1)-2d+2,d]]_q$, where d is a positive integer with $2\le d\le 6t-1$.*

Proof: Let $n=2t(q-1)$ and $r=\frac{q+1}{2t}$. Let $\lambda\in\mathbb{F}_{q^2}$ be a primitive r^{th} root of unity. Noting that every q^2-cyclotomic coset modulo rn contains precisely one element, we assume that $\mathcal{C}_\delta$ is a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set

$$\mathcal{Z}_\delta=\Big\{1+r\Big(-2t+1+i\Big)\,\Big|\,0\le i\le\delta-1\Big\} \tag{IV.6}$$

where δ is a positive integer with $1\le\delta\le 6t-2$. It follows from Lemma IV.4 that $\mathcal{C}_\delta$ is a dual-containing code with parameters $[n,n-d+1,d]$, where d is a positive integer with $2\le d\le 6t-1$. Using the Hermitian construction, we can obtain a quantum MDS code with parameters $[[2t(q-1),2t(q-1)-2d+2,d]]_q$. ∎

Example IV.6. *In Table II, we list some quantum MDS codes obtained from Theorem IV.5.*

C. New quantum MDS codes of length $3(q-1)$

Let q be an odd prime power such that $3^2\mid(q+1)$. Let $n=3(q-1)$ and $r=\frac{q+1}{3}$. Clearly, $r\ge 6$. Let $\lambda\in\mathbb{F}_{q^2}$ be a primitive r^{th} root of unity. Let C be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set

$$Z=\Big\{1+ri\,\Big|-2\le i\le\frac{q-3}{2}\Big\}. \tag{IV.7}$$

It is clear that $0<1+r\big(\frac{q-3}{2}\big)<\frac{q^2-1}{2}$ and $-\frac{q^2-1}{2}<1-2r<0$. Thus, $|Z|=\frac{q+3}{2}$. We show that C is a dual-containing code.

Lemma IV.7. *If C is a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set Z as in (IV.7), then C is a dual-containing code.*

Proof: Suppose otherwise that C is not a dual-containing code. It follows from Lemma II.7 that $Z\bigcap Z^{-q}\neq\emptyset$. Hence, two integers i,j with $-2\le i,j\le\frac{q-3}{2}$ can be found such that

$$-q(1+ri)\equiv 1+rj \pmod{q^2-1}. \tag{IV.8}$$

If $i=j$, then $-q(1+ri)\equiv 1+ri \pmod{q^2-1}$, so $(q-1)\mid(1+ri)$. Let $1+ri=\ell(q-1)$, where ℓ is an integer. Note that $18\mid(q+1)$, and we assume that $q+1=18k$, for some positive integer k. Thus $1+6ki=\ell(18k-2)=18\ell k-2\ell$, which is equivalent to $1=2(9\ell k-\ell-3ki)$. This is a contradiction.

Without loss of generality, we may assume that $i>j$. By Equation (IV.8), $-q(1+ri)\equiv 1+rj \pmod{q-1}$ and $-q(1+ri)\equiv 1+rj \pmod{q+1}$, i.e., $(q-1)\mid\big(r(i+j)+2\big)$ and $(q+1)\mid r(i-j)$. Note that $-2(q-1)<r(i+j)+2<\frac{q+1}{3}(q-1)$ and $0<r(i-j)\le\frac{(q+1)^2}{6}$. Let $r(i+j)+2=\ell_2(q-1)$ and $r(i-j)=\ell_1(q+1)$, where $-1\le\ell_2\le\frac{q+1}{3}-1$ and $1\le\ell_1\le\frac{q+1}{6}$. By $r(i+j)+2=\ell_2(q-1)$, we get $rj=\ell_2(q-1)-2-ri$. Substituting rj into Equation (IV.8) yields $-q(1+ri)\equiv 1+\ell_2(q-1)-2-ri \pmod{q^2-1}$, i.e., $(q-1)ri\equiv-(q-1)(1+\ell_2) \pmod{q^2-1}$. Thus $ri\equiv-(1+\ell_2) \pmod{q+1}$, which implies that $\frac{q+1}{3}\mid(1+\ell_2)$. Since $-1\le\ell_2\le\frac{q+1}{3}-1$, we get $1+\ell_2=0$ or $\frac{q+1}{3}$.

If $1+\ell_2=0$, combining $r(i+j)+2=\ell_2(q-1)$ and $r(i-j)=\ell_1(q+1)$ yields $2rj=-(1+\ell_1)(q+1)$. From $\ell_1\ge 1$, we get $2j=-3(1+\ell_1)\le-6$, which gives $j\le-3$, contradicting our assumption $j\ge-2$.

If $1+\ell_2=\frac{q+1}{3}$, combining $r(i+j)+2=\ell_2(q-1)$ and $r(i-j)=\ell_1(q+1)$ yields $2ri=(\ell_1+\ell_2)(q+1)-2(1+\ell_2)$. Noting that $r=\frac{q+1}{3}$ and $\ell_1\ge-1$, we get $2i=3(\ell_1+\ell_2)-2=3\ell_1+q-4\ge q-1$. It follows that $i\ge\frac{q-1}{2}$, which contradicts our assumption $i\le\frac{q-3}{2}$. ■

Using the Hermitian construction, we have the following quantum MDS codes.

Theorem IV.8. *Let q be an odd prime power such that $3^2\mid(q+1)$. Then, there exists a quantum MDS code with parameters $[[3(q-1),3(q-1)-2d+2,d]]_q$, where d is a positive integer with $2\le d\le\frac{q+5}{2}$.*

Proof: Let $n=3(q-1)$ and $r=\frac{q+1}{3}$. Let $\lambda\in\mathbb{F}_{q^2}$ be a primitive r^{th} root of unity. Recall that every q^2-cyclotomic coset modulo rn contains precisely one element. We assume that $\mathcal{C}_\delta$ is a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set

$$\mathcal{Z}_\delta=\Big\{1+r\Big(-2+i\Big)\Big|\,0\le i\le\delta-1\Big\} \tag{IV.9}$$

where δ is a positive integer with $1\le\delta\le\frac{q+3}{2}$. It follows from Lemma IV.7 that $\mathcal{C}_\delta$ is a dual-containing code with parameters $[n,n-d+1,d]$, where d is a positive integer with $2\le d\le\frac{q+5}{2}$. Using the Hermitian construction, we can obtain a quantum MDS code with parameters $[[2t(q-1),2t(q-1)-2d+2,d]]_q$. ■

Example IV.9. *In Table III, we list some quantum MDS codes obtained from Theorem IV.8.*

q	$[[n,k,d]]_q$	d
17	$[[48,48-2d+2,d]]_{17}$	$2\le d\le 11$
53	$[[156,156-2d+2,d]]_{53}$	$2\le d\le 29$

TABLE III
QUANTUM MDS CODES

D. New quantum MDS codes of length $2^fs(q+1)$

Let q be an odd prime power with $2^e\|(q-1)$ and $s\mid(q-1)$, where e is a positive integer and s is an odd positive integer. Assume that f is an integer satisfying $0\le f<e$. Let $n=2^fs(q+1)$ and $r=2$. It is easy to see that $2n\mid(q^2-1)$, which implies that every q^2-cyclotomic coset modulo $2n$ contains exactly one element. Assume that C is a negacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set

$$Z=\Big\{2i-1\,\Big|\,1\le i\le\frac{q-1}{2}+2^fs\Big\}. \tag{IV.10}$$

It is clear that $|Z|=\frac{q-1}{2}+2^fs$. We show that C is a dual-containing code.

Lemma IV.10. *If C is a negacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set Z as in (IV.10), then C is a dual-containing code.*

Proof: Suppose otherwise that C is not a dual-containing code. It follows from Lemma II.7 that $Z\bigcap Z^{-q}\neq\emptyset$. Hence, two integers i,j with $1\le i,j\le\frac{q-1}{2}+2^fs$ can be found such that $-q(2i-1)\equiv 2j-1 \pmod{2n}$. Expanding this congruence gives

$$j+qi\equiv\frac{q+1}{2} \pmod{n}. \tag{IV.11}$$

Recall that $2^es\mid(q-1)$. We can assume, therefore, that $q-1=2^esc$, where c is a positive integer. From $1\le i\le\frac{q-1}{2}+2^fs$, one gets $1\le i\le 2^fs(2^{e-f-1}c+1)$. Write $i=2^fsu+v$, where u,v are integers with $0\le u\le 2^{e-f-1}c$ and $1\le v\le 2^fs$. By Equation (IV.11), we have

$$j+qv-2^fsu\equiv\frac{q+1}{2} \pmod{n}. \tag{IV.12}$$

We obtain a desired contradiction by considering the following cases:

(i) $0\le u\le 2^{e-f-1}c$ and $1\le v\le 2^fs-1$. In this case, $0<\frac{q+3}{2}=1+q-2^fs\cdot 2^{e-f-1}c\le j+qv-2^fsu\le\frac{q-1}{2}+2^fs+q(2^fs-1)=n-\frac{q+1}{2}<n$. This is a contradiction, since we would obtain $j+qv-2^fsu=\frac{q+1}{2}$ by Equation (IV.12).

(ii) $0\le u\le 2^{e-f-1}c$ and $v=2^fs$. In this case, $i=2^fsu+v=2^fs(u+1)$. By Equation (IV.11), $j\equiv\frac{q+1}{2}+2^fs(u+1) \pmod{n}$. Clearly, $0<j<n$ and $0<\frac{q+1}{2}+2^fs(u+1)\le\frac{q+1}{2}+2^fs\cdot 2^{e-f-1}c+2^fs=q+2^fs\le 2^fs(q+1)=n$. If $\frac{q+1}{2}+2^fs(u+1)=n$, we obtain $j=0$, which is impossible. Thus, we can assume $\frac{q+1}{2}+2^fs(u+1)<n$. It follows that $j=\frac{q+1}{2}+2^fs(u+1)$. However, $\frac{q+1}{2}+2^fs(u+1)\ge\frac{q+1}{2}+2^fs>\frac{q-1}{2}+2^fs\ge j$. This is a contradiction. ■

Using the Hermitian construction, we have the following quantum MDS codes.

Theorem IV.11. *Let q be an odd prime power with $2^e\|(q-1)$ and $s\mid(q-1)$, where e is a positive integer and s is an*

q	$[[n,k,d]]_q$	d
17	$[[72, 72-2d+2, d]]_{17}$	$2 \le d \le 13$
49	$[[600, 600-2d+2, d]]_{49}$	$2 \le d \le 37$

TABLE IV
QUANTUM MDS CODES

odd positive integer. Assume that f is an integer satisfying $0 \le f < e$. Then, there exists a quantum MDS code with parameters $[[2^f s(q+1), 2^f s(q+1)-2d+2, d]]_q$, where d is a positive integer with $2 \le d \le \frac{q+1}{2} + 2^f s$.

Proof: Let $n = 2^f s(q+1)$. Recall that every q^2-cyclotomic coset modulo $2n$ contains precisely one element. We assume that $\mathcal{C}_\delta$ is a negacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set

$$\mathcal{Z}_\delta = \left\{ 2i+1 \,\middle|\, 0 \le i \le \delta - 1 \right\} \qquad \text{(IV.13)}$$

where δ is a positive integer with $1 \le \delta \le \frac{q-1}{2} + 2^f s$. It follows from Lemma IV.10 that $\mathcal{C}_\delta$ is a dual-containing code with parameters $[n, n-d+1, d]$, where d is a positive integer with $2 \le d \le \frac{q+1}{2} + 2^f s$. Using the Hermitian construction, we can obtain a quantum MDS code with parameters $[[2^f s(q+1), 2^f s(q+1)-2d+2, d]]_q$. ■

Note that Theorem IV.11 is a generalization of some results of [25]. Taking $f = 0$ (resp. $f = 1$), [25, Theorem 3.7] (resp. [25, Theorem 3.10]) is an immediate consequence of Theorem IV.11, as stated below.

Corollary IV.12. *Let q be an odd prime power with $s \mid (q-1)$, where s is an odd positive integer. Then, there exists a quantum MDS code with parameters $[[s(q+1), s(q+1)-2d+2, d]]_q$, where d is a positive integer with $2 \le d \le \frac{q+1}{2} + s$.*

Corollary IV.13. *Let q be an odd prime power such that $q \equiv 1 \pmod 4$ and $s \mid (q-1)$, where s is an odd positive integer. Then, there exists a quantum MDS code with parameters $[[2s(q+1), 2s(q+1)-2d+2, d]]_q$, where d is a positive integer with $2 \le d \le \frac{q+1}{2} + 2s$.*

Moreover, taking $2^f s = \frac{q-1}{2}$ in Theorem IV.11, we can obtain q-ary quantum MDS codes of length $\frac{q^2-1}{2}$, which has been given previously in [25, Theorem 3.2].

Corollary IV.14. *Let q be an odd prime power. Then, there exists a quantum MDS code with parameters $[[\frac{q^2-1}{2}, \frac{q^2-1}{2} - 2d+2, d]]_q$, where d is a positive integer with $2 \le d \le q$.*

Example IV.15. *In Table IV, we list some quantum MDS codes obtained from Theorem IV.11.*

V. SUMMARY

Through explicit dual-containing MDS constacyclic codes, we have constructed four new classes of quantum MDS codes using the Hermitian construction of [2]. We summarize in Table V the parameters of all known quantum MDS codes. Classes 17–20 of Table V are the new ones obtained in Section 4.

In Table VI, fixing the value of q yields the value (or range of values) of the length n. We next compare the minimum distances of the new quantum MDS codes of length n with those of previously known ones of the same length. It can be seen that the new quantum MDS codes exhibited here often have minimum distance bigger than what was previously known in the literature, for the same q and length.

Class	q	n	d	d (Class 3)	d (Class 8)	d (Class 12)
17	11	40	7	5	3	-
17	19	72	11	9	3	-
18	7	12	5	3	3	4
18	23	132	17	12	3	12
19	17	48	11	8	3	9
19	53	156	29	26	3	27
20	17	72	13	8	3	-
20	49	600	37	24	3	-

TABLE VI
COMPARISON WITH PREVIOUSLY KNOWN QUANTUM MDS CODES

For example, with $q = 11$ and $h = 3$, Class 17 gives $n = (121-1)/3 = 40$. We then search among Classes 1–16 of Table V to see in which classes can the length 40 be attained. For example, in Class 3, we find $40 = 4 \times 11 - 4$; but in Class 4, there does not exist any positive integer r such that $r \times (11-1) + 1 = 40$. In fact, with $q = 11$, it can be verified that the length 40 can only be attained in Classes 3 and 8. We then compare the largest possible minimum distances of these codes of the same length (as in the row with $q = 11$ in Table VI).

ACKNOWLEDGMENT

The authors thank the Associate Editor and the anonymous reviewers for their constructive comments and suggestions. The research of Bocong Chen and San Ling is partially supported by Nanyang Technological University's research grant number M4080456. The research of Guanghui Zhang is supported by NSFC (Grant No. 11171370), the Youth Backbone Teacher Foundation of Henan's University (Grant No. 2013GGJS-152), and Science and Technology Development Program of Henan Province in 2014 (144300510051).

REFERENCES

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "On quantum and classical BCH codes," IEEE Trans. Inf. Theory, vol. 53, no. 3, pp. 1183-1188, Mar. 2007.

[2] A. Ashikhmin and E. Knill, "Nonbinary quantum stablizer codes," IEEE Trans. Inf. Theory, vol. 47, no. 7, pp. 3065-3072, Nov. 2001.

[3] A. Ashikhmin and S. Litsyn, "Foundations of quantum error correction," Recent Trends in Coding Theory and Its Applications, 2007.

[4] A. Ashikhmin, M. A. Tsfasman, and S. Litsyn, "Asymptotically good quantum codes," Phys. Rev. A, vol. 63, pp. 032311-1-032311-5, Feb. 2001.

[5] N. Aydin, I. Siap, and D. J. Ray-Chaudhuri, "The structure of 1-generator quasi-twisted codes and new linear codes," Designs, Codes and Crypt., vol. 24, pp. 313-326, Dec. 2001.

[6] J. Bierbrauer and Y. Edel, "Quantum twisted codes," J. Comb. Designs, vol. 8, pp. 174-188, 2000.

[7] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over $GF(4)$," IEEE Trans. Inf. Theory, vol. 44, no. 4, pp. 1369-1387, Jul. 1998.

[8] H. F. Chau, "Five quantum register error correction code for higher spin systems," Phys. Rev. A, vol. 56, pp. R1-R4, Jul. 1997.

[9] B. Chen, Y. Fan, L. Lin, and H. Liu, "Constacyclic codes over finite fields," Finite Fields Appl., vol. 18, pp. 1217-1231, 2012.

$Class$	Length	Distance	Reference
1	$n \leq q+1$	$d \leq \lfloor n/2 \rfloor + 1$	[13], [15], [33]
2	$mq - l$ $0 \leq l < m, 1 < m < q$	$d \leq m - l + 1$	[30], [34]
3	$mq - l$ $0 \leq l \leq q-1, 1 \leq m \leq q$	$3 \leq d \leq (q+1-\lfloor l/m \rfloor)/2$	[21]
4	$r(q-1)+1$ $q+1 \equiv r \pmod{2r}$	$d \leq (q+r+1)/2$	[22]
5	$q^2 - s$ $0 \leq s < q/2 - 1$	$q/2+1 < d \leq q - s$	[22]
6	$(q^2+1)/2 - s$ $0 \leq s < q/2 - 1$	$q/2+1 < d \leq q - s$	[22]
7	$(q^2+1)/2$, q odd	$3 \leq d \leq q$, d odd	[24]
8	$4 \leq n \leq q^2+1$ $q \neq 2$ and $n \neq 4$	3	[6], [21], [29]
9	$q^2 - l$	$d \leq q - l, 0 \leq l \leq q-2$	[15], [30]
10	q^2+1	$2 \leq d \leq q+1$	[21], [22], [24], [17]
11	$(q^2-1)/2$, q odd	$2 \leq d \leq q$	[25]
12	$\frac{q^2-1}{r}$, q odd $r \mid (q+1)$, r even and $r \neq 2$	$2 \leq d \leq (q+1)/2$	[25]
13	$\lambda(q+1)$, q odd λ odd, $\lambda \mid (q-1)$	$2 \leq d \leq (q+1)/2 + \lambda$	[25]
14	$2\lambda(q+1)$, $q \equiv 1 \pmod 4$ λ odd, $\lambda \mid (q-1)$	$2 \leq d \leq (q+1)/2 + 2\lambda$	[25]
15	$(q^2+1)/5$, $q = 20m+3$ or $20m+7$	$2 \leq d \leq (q+5)/2$, d even	[25]
16	$(q^2+1)/5$, $q = 20m-3$ or $20m-7$	$2 \leq d \leq (q+3)/2$, d even	[25]
17	$n = \frac{q^2-1}{h}$, q odd, $h \mid (q+1)$, $h \in \{3,5,7\}$	$2 \leq d \leq \frac{(q+1)(h+1)}{2h} - 1$	**New**
18	$n = 2t(q-1)$, $8 \mid (q+1)$, $t \mid (q+1)$, t odd	$2 \leq d \leq 6t - 1$	**New**
19	$n = 3(q-1)$, $3^2 \mid (q+1)$ q odd	$2 \leq d \leq \frac{q+5}{2}$	**New**
20	$2^f s(q+1)$, $2^e \| (q-1)$ $0 \leq f < e$, $s \mid (q-1)$, s odd	$2 \leq d \leq \frac{q+1}{2} + 2^f s$	**New**

TABLE V
QUANTUM MDS CODES

[10] H. Chen, S. Ling, and C. Xing, "Quantum codes from concatenated algebraic-geometric codes," IEEE Trans. Inf. Theory, vol. 51, no. 8, pp. 2915-2920, Aug. 2005.

[11] G. Cohen, S. Encheva, and S. Litsyn, "On binary constructions of quantum codes," IEEE Trans. Inf. Theory, vol. 45, no. 7, pp. 2495-2498, Nov. 1999.

[12] D. G. Cory, M. D. Price, W. Maas, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, and S. S. Somaroo, "Experimental Quantum Error Correction," Phys. Rev. Lett., vol. 81, pp. 2152-2155, Sep. 1998.

[13] K. Feng, "Quantum codes $[[6,2,3]]_p$ and $[[7,3,3]]_p$ $(p \geq 3)$ exist," IEEE Trans. Inf. Theory, vol. 48, no. 8, pp. 2384-2391, Jan. 2002.

[14] K. Feng, S. Ling, and C. Xing, "Asymptotic bounds on quantum codes from algebraic geometry codes," IEEE Trans. Inf. Theory, vol. 52, no. 3, pp. 986-991, Mar. 2006.

[15] M. Grassl, T. Beth, and M. Rötteler, "On optimal quantum codes," Int. J. Quantum Inform., vol. 2, no. 1, pp. 757-766, Mar. 2004.

[16] G. G. La Guardia, "Constructions of new families of nonbinary quantum codes," Phys. Rev. A, vol. 80, no. 4, pp. 042331-1-042331-11, Oct. 2009.

[17] G. G. La Guardia, "New quantum MDS codes," IEEE Trans. Inf. Theory, vol. 57, no. 8, pp. 5551-5554, Aug. 2011.

[18] G. G. La Guardia and R. Palazzo, "Constructions of new families of nonbinary CSS codes," Discrete Math., vol. 310, no. 21, pp. 2935-2945, 2010.

[19] M. Hamada, "Concatenated quantum codes constructible in polynomial time: efficient decoding and error correction," IEEE Trans. Inf. Theory, vol. 54, no. 12, pp. 5689-5704, Dec. 2008.

[20] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.

[21] L. Jin, S. Ling, J. Luo, and C. Xing, "Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes," IEEE Trans. Inf. Theory, vol. 56, no. 9, pp. 4735-4740, Sep. 2010.

[22] L. Jin and C. Xing, "A construction of new quantum MDS codes," IEEE Trans. Inf. Theory, vol. 60, no. 5, pp. 2921-2925, Aug. 2014.

[23] L. Jin and C. Xing, "Euclidean and Hermitian self-orthogonal algebraic geometry codes and their application to quantum codes," IEEE Trans. Inf. Theory, vol. 58, no. 8, pp. 5484-5489, Aug. 2012.

[24] X. Kai and S. Zhu, "New quantum MDS codes from negacyclic codes," IEEE Trans. Inf. Theory, vol. 59, no. 2, pp. 1193-1197, 2013.

[25] X. Kai, S. Zhu, and P. Li, "Constacyclic codes and some new quantum MDS codes," IEEE Trans. Inf. Theory, vol. 60, no. 4, pp. 2080-2086, 2014.

[26] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," IEEE Trans. Inf. Theory, vol. 52, no. 11, pp. 4892-4914, Nov. 2006.

[27] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," Phys. Rev. A, vol. 55, no. 2, pp. 900-911, Feb. 1997.

[28] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," Phys. Rev. Lett., vol. 77, no. 1, pp. 198-201, Jul. 1996.

[29] R. Li and Z. Xu, "Construction of $[[n, n-4, 3]]_q$ quantum codes for odd prime power q," Phys. Rev. A, vol. 82, pp. 052316-1-052316-4, Nov. 2010.

[30] Z. Li, L. J. Xing, and X. Wang, "Quantum generalized Reed-Solomon codes: Unified framework for quantum maximum-distanceseparable codes," Phys. Rev. A, vol. 77, pp. 012308-1-012308-4, Jan. 2008.

[31] S. Ling, L. Luo, and C. Xing, "Generalization of Steane's enlargement construction of quantum codes and applications," IEEE Trans. Inf. Theory, vol. 56, no. 8, pp. 4080-4084, Aug. 2010.

[32] M. D. Reed, L. Dicarlo, S. E. Nigg, L. Sun, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf, "Realization of three-qubit quantum error correction with superconducting circuits," Nature, vol. 482, pp. 382-385, Feb. 2012.

[33] M. Rötteler, M. Grassl, and T. Beth, "On quantum MDS codes," In Proc. Int. Symp. Inf. Theory, Chicago, USA, pp. 356, 2004.

[34] P. K. Sarvepalli and A. Klappenecker, "Nonbinary quantum Reed-Muller codes," In Proc. Int. Symp. Inf. Theory, Adelaide, Australia, pp. 1023-1027, 2005.

[35] A. M. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," IEEE Trans. Inf. Theory, vol. 45, no. 11, pp. 2492-2495, Nov. 1999.

[36] A. M. Steane, "Quantum Reed-Muller codes," IEEE Trans. Inf. Theory, vol. 45, no. 5, pp. 1701-1703, Jul. 1999.

[37] Y. Yang and W. Cai, "On self-dual constacyclic codes over finite fields," Designs, Codes and Crypt., DOI: 10.1007/s10623-013-9865-9, 2013.

Bocong Chen received his Ph.D. degree in mathematics from Central China Normal University in 2013. He is currently a Research Fellow in the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. His research interests include classical error-correcting codes and quantum error-correcting codes.

San Ling received the B.A. degree in mathematics from the University of Cambridge in 1985 and the Ph.D. degree in mathematics from the University of California, Berkeley in 1990. Since April 2005, he has been a Professor with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, in Nanyang Technological University, Singapore. Prior to that, he was with the Department of Mathematics, National University of Singapore. His research fields include arithmetic of modular curves and applications of number theory to combinatorial designs, coding theory, cryptography and sequences.

Guanghui Zhang received his Ph.D. degree in mathematics from Central China Normal University in 2010. He is currently an Associate Professor in the School of Mathematical Sciences, Luoyang Normal University, China. His main research interests cover classical error-correcting codes, codes over rings and quantum error-correcting codes.